## REMARKS

Claim 1 has have been amended.

Claim Rejections – 35 U.S.C. §103

The Examiner rejected claims 1-20 under 35 USC 103 as being unpatentable over Easter (5,530,749) and Elgamal (5,657,390). Applicant respectfully disagrees with the Examiner's rejection. In particular, both Easter and Elgamal, alone or in communication, fail to teach or suggest a receiving a key associated with an encrypted code defining a unique hardware configuration based upon the decrypted key to establish a unique hardware configuration.

In particular, as noted in the application, the re-configurable feature of the IHAD allows the hardware to be changed at regular intervals, thus circumventing any attempts at compromising the hardware. For example, a new hardware configuration could be used everyday, or even every transaction. An encrypted external message (e.g., real time video) may be downloaded off the Internet from a source. The encrypted external message, which may be stored in system memory 14 once it is downloaded, is typically encrypted utilizing a public key/private key or other conventional secure method. *Prior to decrypting the message, an encrypted hardware configuration code associated with the encrypted external message is provided to the chipset 16 from the source.* In particular, as noted in the application on page 2, line 24-page 3, line 2:

> The present invention provides an inferred hardware assisted decryption (IHAD) electronic system 10 that utilizes a re-configurable hardware block in conjunction with a processor running a software decryption algorithm that determines the form of the hardware. The re-configurable feature of the IHAD allows the hardware to be changed at regular intervals, thus circumventing any attempts at compromising the hardware. For example, a new hardware configuration could be used everyday, or even every transaction. As a result, by the time the hardware is compromised, it is no longer being used. The speed benefits of a hardware only type of decryption can thus be realized.

Furthermore, as shown on page 4, line 22- page 5, line 16:

For illustrative purposes, the operations of the IHAD electronic system 10 are discussed in relation to the receipt of an encrypted external message, such as an encrypted external message (e.g., real time video) downloaded off the Internet from a source. The encrypted external message, which may be stored in system memory 14 once it is downloaded, is typically encrypted utilizing a public key/private key or other conventional secure method.

Prior to decrypting the message, an encrypted hardware configuration code associated with the encrypted external message is provided to the chipset 16 from the source. The CPU 12, in communication with the chipset 16, decrypts the encrypted hardware configuration code using a local key. The key is extracted from the message by decrypting the message with a key contained in the memory 30 of the chipset 16. The key may be a private key associated with the electronic system 10 if public/private key cryptography is used to secure communication between the IHAD electronic system 10 and other networked systems.

The CPU 12 thus processes the hardware configuration code using a key to which it has access. The public and/or private key used during the initial decryption phase could be held in the memory 30, typically in a non-volatile RAM although a volatile RAM could be used as well. Alternatively, the key could be held in the CPU's ROM or RAM, depending on the requirements of the application. The configuration logic 28 assists the CPU 12 in configuring the programmable array of gates 18.

The CPU 12 thus reads the key, decodes the message and runs a software decryption algorithm that will determine the unique configuration of the hardware. By determining the unique configuration of the hardware, the CPU 12 configures the hardware itself via the programmable array of gates 18. After the encrypted hardware configuration code is decoded, the CPU 12 sends command signals through the configuration logic 28 into the programmable array of gates 18 for reconfiguring the hardware. The configuration logic 28 assists the CPU 12 in configuring the programmable array of gates 18. The memory interface block 34 interfaces the programmable array of gates 18 to the remaining chipset logic 32 and system memory 14. One skilled in the art will recognize that the programmable array of gates 18 can be reconfigured in a conventional manner, for example, by adjusting the wiring of the gates, flip-flops and so forth.

Both Easter and Elgamal, alone or in communication, fail to teach or disclose receiving a message that includes an encrypted hardware configuration code for configuring the hardware. Hardware can thus not be changed at regular intervals or even every transaction as in embodiments of the present invention. Rather, Easter just relies on comparing a key code to a secure code on the computer chip. An encrypted hardware code is not received and then decrypted.

Furthermore, both Easter and Elgamal, alone or in combination, fail to teach or suggest decrypting the encrypted hardware configuration code using a local key. Embodiments of the invention provide a key that is extracted from the message by decrypting the message with a key contained in the memory 30 of the chipset 16. The CPU 12 thus reads the key, decodes the message and runs a software decryption algorithm that will determine the unique configuration of the hardware. By determining the unique configuration of the hardware, the CPU 12 configures the hardware itself via the programmable array of gates 18.

Easter teaches away from this as well in that there is no decryption of a hardware configuration code performed. Rather the key code is merely compared to a secure code.

## CONCLUSION

In view of the foregoing, it is respectfully asserted that all of the claims pending in this patent application are in condition for allowance.

The required fee for a two month extension of time is enclosed. Should it be determined that an additional fee is due under 37 CFR §§1.16 or 1.17, or any excess fee has been received, please charge that fee or credit the amount of overcharge to deposit account #02-2666.

If the Examiner has any questions, he is invited to contact the undersigned at (323) 654-8218. Reconsideration of this patent application and early allowance of all the claims is respectfully requested.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

Dated: December 30, 2004

By _____
Farzad E. Amini, Reg. No. 42,261

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, Post Office Box 1450, Alexandria, Virginia 22313-1450 on December 30, 2004.

_____
*Margaux Rodriguez* *December 30, 2004*